



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 23 January 2004

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Star–Telegram reports American Airlines and U.S. safety regulators say they're closely monitoring developments at a Japanese airline that is having a rash of problems with MD–80–series aircraft engines. (See item [10](#))
- The Durham Herald Sun reports Pittsboro, NC, is telling residents to boil their water or not use it all after finding E.Coli bacteria in the water supply. (See item [16](#))
- earthweb.com reports Cisco has warned of a default installation vulnerability in multiple voice products running on the IBM platform that leaves TCP and UDP ports open to malicious attack. (See item [24](#))
- eSecurityPlanet reports Sun Microsystems on Wednesday, January 21, warned that systems running Sun Cluster 3.x with SunPlex Manager configured were at risk of takeover because of known flaws in the OpenSSL protocol. (See item [26](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – <http://esisac.com>]

January 22, Reuters — **FERC approves natural gas pipeline.** The Federal Energy Regulatory Commission on Thursday, January 22, gave final approval to AES Corp.'s Ocean Express pipeline project to ship natural gas from the Bahamas to southeastern Florida. The 54-mile pipeline would transport up to 842 million cubic feet of natural gas a day. The pipeline would connect with the Florida Gas Transmission Co. pipeline system in Broward County, FL. The Ocean Express pipeline would connect with, and receive natural gas transported by, a 40-mile Bahamian-jurisdiction pipeline that extends to Ocean Cay, Bahamas. Ocean Cay, a 90-acre man-made industrial island, would be the site of a liquefied natural gas (LNG) storage and regasification facility that would receive LNG from foreign suppliers.
Source: http://biz.yahoo.com/rc/040122/energy_pipeline_1.html

2. *January 21, Dow Jones Business News* — **New York City must add megawatts by 2008.** New York City's energy task force said Wednesday, January 21, the city will need 2,600 MW of new electric supply by 2008 to meet growing demand. The 16-member group released a report with more than two dozen specific recommendations for improving energy efficiency, increasing generation and transmission capacity, and improving the city's electric distribution system. The task force recommended lobbying the state legislature to amend and revive the expired power plant siting law, in an effort to provide certainty and encourage investment in new power plants. It said it also supported innovative financing for electric projects, including the use of long-term power purchase agreements as a vehicle for reducing project risk. Additionally, the group suggested expanding the city's energy efficiency programs and establishing a formal planning process to coordinate the development of major projects for the city, state and local utilities.
Source: http://biz.yahoo.com/djus/040121/1736001486_1.html

[\[Return to top\]](#)

Chemical Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

3. *January 22, Baltimore Sun (MD)* — **Army big enough to do the job according to Rumsfeld.** Secretary of Defense Donald H. Rumsfeld dismissed on Wednesday, January 21, any contention that the Army is too small to meet its worldwide commitments, pointing out that he has used his emergency powers to temporarily boost the size of the force. "We've increased end strength substantially," said Rumsfeld, using the service term for the total number of soldiers. The overall increase is about 36,000 troops, accomplished through the Pentagon's emergency order that temporarily bars service members from completing their enlistments or retiring until they finish their duty in Iraq or Afghanistan. Rumsfeld has said repeatedly that the Army is large enough with its current 480,000 troops to accomplish its missions in Iraq, Afghanistan and elsewhere when the emergency retention measures are taken into account. The Army's size is set by Congress.
Source: <http://www.sunspot.net/news/nationworld/bal-te.pentagon22jan>

4. *January 21, Federal Computer Week* — **Netcentric warfare to use more simulations. Training soldiers to take advantage of network-centric warfare will require more simulations, training sessions and war games in coming years, according to senior Department of Defense leadership. As the military becomes a more networked force, it will have to relearn how to fight, and simulations and war games will be the most effective and efficient means of doing so, said Navy Adm. Edmund Giambastiani, commander of U.S. Joint Forces Command (JFCOM). "We need to increase the scope, speed, breadth and depth of our training operations," Giambastiani said. The services and JFCOM are planning numerous training and war game operations this year. Giambastiani lauded the use of such facilities as the Joint National Training Capability, a global network of training facilities. He said JFCOM will conduct three war games this year to study more aspects of joint warfighting. One exercise that the Air Force will be running is the Joint Expeditionary Force Experiment (JEFX) 2004 in August. JEFX is a series of experiments that combine live-fly, live-play, ground and naval forces, simulations and technology insertion into a warfighting environment. Source: <http://www.fcw.com/fcw/articles/2004/0119/web-sims-01-21-04.asp>**

[[Return to top](#)]

Banking and Finance Sector

5. *January 22, Associated Press* — **Identity theft tops consumers' complaints. Reports of Internet-related fraud now account for more than half the consumer complaints filed with the Federal Trade Commission (FTC), the agency said Thursday, January 22. Internet-related fraud was the subject of 55 percent of the more than half-million complaints filed in 2003, up from 45 percent a year earlier, the FTC said. The median loss for victims of Internet-related fraud was \$195. Identity theft — stealing someone's personal information for financial gain — was the most common complaint the FTC received for the fourth consecutive year, the agency said. It represented 42 percent of all complaints in 2003, up from 40 percent the year before. The most common cases of identity theft involved credit cards, followed by telephones or utilities, banks, and workplace fraud. However, concern was growing about online transactions of any kind. Internet auctions represented 15 percent of the complaints, while shop-at-home/catalog sales were nine percent, and Internet services and computer complaints made up six percent. The report highlighted data from Consumer Sentinel, the complaint database developed and maintained by the FTC, and the Identity Theft Data Clearinghouse. Report: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf> Source: http://seattlepi.nwsourc.com/business/apbiz_story.asp?category=1310&slug=Consumer%20Complaints**
6. *January 22, Associated Press* — **Asset freeze requested. The United States and Saudi Arabia are asking the United Nations to freeze the assets of four branches of a Saudi charity accused of financially supporting Osama bin Laden's al Qaeda terror network, authorities announced Thursday, January 22. The four branches of the charity, Al-Haramain Islamic Foundation, are located in Indonesia, Kenya, Tanzania and Pakistan, the Department of Treasury said. "These branches have provided financial, material and logistical support to the al Qaeda network and other terrorist organization," the department**

said. Also Thursday, the United States said it was adding the four branches to its own list of people and groups suspected of financially supporting terrorism. That means any financial assets belonging to the branches found in this country must be frozen. It also means the designated branches are cut off from the United States' financial system.

Source: <http://www.washingtonpost.com/ac2/wp-dyn/A38378-2004Jan22>

[\[Return to top\]](#)

Transportation Sector

7. *January 22, Transport Topics News* — **DOT plans to require Hazmat haulers to provide communications systems for drivers. The Department of Transportation (DOT) plans to require hazardous materials haulers to provide communications systems for drivers to ensure the safety of their loads, an official of the Research and Special Programs Administration told a transportation forum in Washington, D.C. last week.** Speaking on hazardous materials regulation before a session of the annual meeting of the Transportation Research Board, Douglas Reeves, a RSPA engineer, said the agency was studying requiring both simple and "more elaborate" communications systems for drivers. Speaking only in general terms, Reeves said, "There are two categories. One is [like a] cell phone that will give them some way to communicate."

Source: <http://www.ttnews.com/members/topnews/0011052.html>

8. *January 22, The Trucker* — **Fatal crash rate for large trucks drops 11 percent. Highway safety for the trucking industry continues to show improvement, according to new information released by the Department of Transportation (DOT).** DOT information showed that the 2002 fatal crash rate for large trucks is 1.9 fatal crashes per 100 million vehicle miles traveled. This is an 11 percent reduction from the previous year, according to the American Trucking Associations (ATA), and puts the rate at its lowest point since the DOT began keeping large truck safety records in 1975. "The trucking industry and our drivers continue to work hard every mile, every day to make our highways safer," said Bill Graves, president of ATA in a news release. "Their commitment is making a difference." ATA stated that the large truck fatal crash rate coincides with a reduction in the number of truck-involved highway fatalities for the fifth year in a row with trucking as the only group to show a decline in 2002.

Source: http://www.thetrucker.com/stories/01_04/0122_fatal_rate.htm

9. *January 22, Business Times (Singapore)* — **Security standards for sky marshals needed: BA chief. British Airway's (BA) chief executive Rod Eddington said on Tuesday, January 20, it may be appropriate to put sky marshals aboard an airliner to prevent hijackings, but that standards must be set to make sure it is done safely.** The United States announced on December 29 that it would require armed law enforcement officers to be placed aboard international flights in U.S. airspace when necessary, a demand that some European nations have balked at. **Britain and France are open to the idea of sky marshals, but Finland, Portugal, Sweden and Denmark have signaled they prefer canceling flights to deploying armed guards on planes if there were a strong suspicion of an attack.** Such protocols were the subject of a visit last week to Brussels by Asa Hutchinson, U.S. undersecretary for border and transportation security.

Source: <http://business-times.asia1.com.sg/story/0.4567.105995.00.ht ml>

10. *January 22, Star-Telegram (Japan)* — **Japanese airline grounds flights. American Airlines and U.S. safety regulators said Wednesday, January 21, that they're closely monitoring developments at a Japanese airline that is having a rash of problems with MD-80-series aircraft engines.** Japan Air System was forced to ground most of its 25 MD-80-series jets in recent days for emergency inspections after discovering cracked engine parts. The inspections were undertaken after two of the aircraft had engine vibration problems and had to abort flights on successive days. **American, with 335 of the twin-engine, single-aisle jets, is the world's largest operator of MD-80s.** "We're monitoring the situation closely, but at this time we're not being told to do any inspections," American spokesman John Hotard said. Federal Aviation Administration (FAA) spokesman Paul Turk said the agency has not seen evidence to justify ordering U.S. airlines to undertake any additional engine inspections. The FAA, Turk said, is awaiting further information from engine manufacturer Pratt & Whitney, which is investigating the problems with the widely used JT8D-series engines. The Japanese airline grounded more than 200 flights through Wednesday while it inspected its MD-80s. Pratt & Whitney spokesman Mark Sullivan said the airline had discovered minute cracks in compressor vanes, small welded pieces of steel that direct the airflow into the jet engine compressor.

Source: <http://www.dfw.com/mld/dfw/business/7769372.htm>

11. *January 21, Department of Transportation* — **U.S. Transportation Secretary Mineta announces congestion relief for Chicago's O'Hare International.** Transportation Secretary Norman Y. Mineta Wednesday, January 21, announced the signing of an order that will significantly reduce flight congestion and passenger inconvenience at Chicago's O'Hare International Airport. **Under terms of the order signed by Federal Aviation Administrator Marion Blakey and accepted by both airlines, American and United have agreed to reduce by five percent those carriers, operations during the peak hours between 1 p.m. and 8 p.m. This reduction of 62 scheduled flights, which takes effect in early March and lasts for six months,** returns scheduled O'Hare operations to October 2003 levels, the last month prior to significant delays. "Today's announcement is a significant, first step toward getting planes into and out of Chicago on time," said Secretary Mineta. "While this Department continues working toward a comprehensive, long-term solution to this challenge, this order provides American travelers with necessary and immediate action to alleviate potential travel delays."

Source: <http://www.dot.gov/affairs/dot0304.htm>

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

12.

January 22, Oster Dow Jones Commodity News — **USDA crafting ways to test more downer cattle.** The U.S. Department of Agriculture (USDA) is crafting methods to increase testing of non-ambulatory cattle in the wake of having a cow test positive for bovine spongiform encephalopathy (BSE), now that all such cattle are banned from the human food chain, Agriculture Secretary Ann Veneman told the House Agriculture Committee. **Since the ban on downer cattle was put in place December 30, questions have arisen about how those animals will be tested since they are not taken to a federally inspected slaughter facility. Many are concerned that they will slip through the cracks and never be tested and that the USDA's testing program would miss cattle that have BSE.** House Agriculture Committee members expressed these concerns home with repeated questions to Veneman. She responded by saying the USDA is working to step up contact with U.S. veterinarians and with rendering plants to make those animals available for testing. Many of the dead or dying cattle that currently go to a rendering facility without being tested for BSE could be presented to a veterinarian for testing under the new system. There also would be appeals to cattlemen to allow testing of dead animals that aren't going to rendering, Veneman said.

Source: http://www.agprofessional.com/show_story.php?id=23211

13. *January 22, USAgNet* — **USDA BSE investigation expands to Oregon.** The U.S. Department of Agriculture (USDA) said on Wednesday, January 21, its investigation into the first U.S. case of bovine spongiform encephalopathy (BSE) has expanded to Oregon, after linking a cow there to the infected animal in Washington state. **The USDA said a dairy facility near the Washington state border in Boardman, Oregon, was placed under state quarantine after a cow was determined to be in the same herd as the Holstein dairy cow diagnosed with BSE on December 23.** USDA investigators are still searching for several dozen cattle that were in the same herd as the infected cow when it was born on an Alberta, Canada, dairy farm. As many as 98 animals were raised together in Canada, which means they may have shared the same source of feed, and then sent to the U.S. in two shipments in 2001. The USDA said it has yet to locate 71 of the animals. **Six herds in Washington state have also been quarantined because of links with the infected cow.**

Source: <http://www.usagnet.com/story-national.cfm?Id=72&yr=2004>

[\[Return to top\]](#)

Food Sector

14. *January 22, Associated Press* — **Japan forbids imports of Thai chicken.** Japan, Thailand's largest poultry export market, on Thursday, January 22, banned imports of Thai chicken in response to the first reported human case of bird flu in Thailand, agricultural officials said. In Bangkok, the Thai prime minister, Thaksin Shinawatra, denied that a laboratory had confirmed a case of the illness in Thailand's central Suphanburi Province. The Japanese government reacted quickly. "We suspended as of today," a Japanese Agriculture Ministry official said of the imports. "We have not confirmed the infection but cannot rule it out either," the official said. **Thailand exported 540,000 tons of chicken last year, half of it to Japan, according to industry data.** The European Union is the second largest importer of Thai chicken, and the EU executive said Thursday that it was watching the situation closely and could ban imports if a human outbreak was proved in Thailand.

Source: <http://www.iht.com/articles/126104.htm>

Water Sector

15. *January 22, Water Tech Online* — **Demand outstripping water resources. Water disputes in the western United States may continue to escalate unless the water industry understands that water supply is no longer driven solely by drought, it's impacted even in times of normal precipitation,** the American Water Works Association (AWWA) reported. This message was delivered January 19, by Bennett Raley, assistant U.S. Department of Interior secretary for water and science, to attendees of AWWA's Water Sources Conference and Exposition. Addressing the opening general session, Raley discussed his agency's Water 2025 plan that offers new strategies to combat ongoing and future water shortages in the western United States. **Raley said that shortages will occur even in normal precipitation years.** The agency's Water 2025 plan includes several tools to help the appropriate parties ensure adequate future supplies for the future including promoting conservation; efficiency and market-based plans; working collaboratively with other stakeholders to resolve conflicts; and using improved technology for getting and spreading information.

Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=45543

16. *January 22, Durham Herald Sun* — **Pittsboro residents told to boil water. Pittsboro, NC, is telling residents to boil their water or not use it all after finding E.Coli bacteria in the water supply.** The bacteria finding means that the water might be contaminated with human or animal waste. The bacteria was isolated from one sampling point in the city supply. The town health department is currently collecting additional samples, increasing disinfectant in the supply, and flushing the system. Meanwhile, the health department is recommending to residents that they use bottled water, discard raw vegetables or fruits previously prepared, and not drink from water fountains or coolers.

Source: <http://www.herald-sun.com/chatham/13-438298.html>

Public Health Sector

17. *January 22, Agence France Presse* — **Spread of bird flu fuels fears of mutation. The World Health Organization (WHO) said Wednesday, January 21, that it was concerned the H5N1 strain of bird flu was spreading across Asia and providing mounting opportunities for it to mutate into a far more lethal virus.** The warning came after claims by a Thai politician that a seven-year-old boy in Thailand had contracted the potentially fatal disease and that two other people were being tested for infection. **"The spread of the virus is so wide across such a large part of Asia that we see there is a reason for growing concern,"** said Bob Dietz, the WHO's spokesman in Vietnam. "The more widespread it becomes the more chance there is that it could alter its form." At least five people have died from the virus in Vietnam, while 17 others suspected of contracting it remain in hospital. Japan, South Korea, and Taiwan are battling their own outbreaks, but have not reported any cases of human infection.

Source: <http://www.smh.com.au/articles/2004/01/22/1074732543027.html>

18. *January 22, Associated Press* — **Thai boy has bird flu, lawmaker says. After days of denying it had a problem, Thailand became the latest flashpoint in the bird flu crisis with claims Thursday, January 22, that a village boy is infected.** In Bangkok, Thai Prime Minister Thaksin Shinawatra denied claims that the country's first bird flu case in humans had been confirmed by a laboratory. But a Thai senator, Nirun Phitakwatchara said a boy has tested positive for the disease. Thailand is among the world's top five poultry exporters and stocks in its multibillion-dollar industry dropped as much as seven percent on the Stock Exchange of Thailand. The government has repeatedly insisted that it has not been hit by bird flu, saying that the six million chickens that have died or been destroyed in central Thailand were infected with bird cholera and other respiratory diseases. **The sick boy is one of three people being tested for bird flu in Thailand.** Health officials believe that the disease is contracted through contact with sick birds.

Source: http://abcnews.go.com/wire/Living/ap20040122_905.html

19. *January 22, American Chemical Society* — **Bacterium may lead to better anti-viral vaccines. A new vaccine formulation that utilizes an unusual protein derived from a bacterium that causes food poisoning, Listeria, could be used to improve the safety and effectiveness of vaccines for a variety of viral diseases. These could include HIV, smallpox, and influenza, according to researchers at the University of Michigan.** Conventional vaccine formulations typically use live or weakened viruses to boost the immune response. The Listeria formulation uses viral protein components along with the bacterial protein, reducing the possibility of accidental viral infection. In preliminary animal studies, the new vaccine also appeared to boost the immune response better than a conventional vaccine, according to the researchers. The vaccine incorporates a bacterial protein called listeriolysin O (LLO), which has the unusual ability to allow Listeria to cut through and enter certain cells that are involved in the immune response. These cells, called macrophages, are in turn able to activate other immune cells called cytotoxic T-lymphocytes, which are needed for complete protection against viral diseases but are not adequately activated by conventional vaccine formulations.

Source: http://www.eurekalert.org/pub_releases/2004-01/acs-tc012104.php

20. *January 22, U.S. Army Medical Research Institute of Infectious Diseases* — **Small-molecule inhibitors of anthrax lethal factor identified. Scientists, from the U.S. Army Medical Research Institute of Infectious Diseases and colleagues, have identified several compounds that block the activity of a key anthrax protein called lethal factor (LF), an important first step in developing therapeutics to counter the disease.** Anthrax toxin consists of three proteins: lethal factor, protective antigen, and edema factor, all of which work in concert to kill host cells. While the exact mechanism of anthrax toxin is not yet well understood, it is clear that developing methods to inhibit toxin assembly and/or function is critically important. Using a two-stage screening assay, researchers identified a number of compounds that inhibited the activity of LF. All inhibitors were further verified by high-performance liquid chromatography and their efficacy was validated in cell culture. Finally, molecular modeling techniques were used to predict structural features that contribute to inhibitor binding and potency. These techniques revealed a common pharmacophore upon which future therapeutics can be built. This pharmacophore will serve as a basis for directing future efforts to develop LF inhibitors with enhanced potency.

[\[Return to top\]](#)

Government Sector

21. *January 22, The White House* — **Progress in the War on Terror – Bush budget raise DHS.** The President on Thursday, January 22, announced a 9.7% increase in government-wide homeland security funding in his FY 2005 budget, nearly tripling the FY 2001 levels (excluding the Department of Defense and Project BioShield). The President's budget will propose increasing counterterrorism funding through the Department of Justice to \$2.6 billion, a 19% increase over FY 2004 levels. The additional Department of Justice resources will put more FBI agents to work on counterterrorism activities, bringing overall FBI funding to \$5.1 billion — a \$1.9 billion (60%) increase over FY 2001 levels. The additional resources will also strengthen the FBI's intelligence capabilities and support the interagency Terrorist Threat Integration Center, announced by President Bush in last year's State of the Union Address. Since 2001, the Federal government has provided more than \$13 billion to help state and local governments prepare for terrorism.

Source: <http://www.whitehouse.gov/news/releases/2004/01/20040122-1.h tml>

22. *January 22, Federal Computer Week* — **Conference of Mayors: Cities not getting DHS grants .** Regional planning and cooperation are the hallmarks of programs in which federal funding for homeland security has been used effectively — but most cities still haven't received federal dollars provided to first responders for homeland security, according to officials at the U.S. Conference of Mayors (USCM). **A new study conducted by the USCM, to be released later Thursday, January 22, shows that at least 75 percent of cities have not seen money from grants that the Homeland Security Department has already awarded to state and local agencies,** said Martin O'Malley, mayor of Baltimore and co-chairman of the organization's Homeland Security Task Force. Mayors would like to see more emphasis from the Department of Homeland Security (DHS) on regional efforts that cross cities, counties and states, largely because of the shortfalls faced by smaller cities and towns, said David Wallace, mayor of Sugar Land, Texas and co-chairman of the task force. States where funding is going where it's needed, such as Florida and Mississippi, have adopted a regional structure, said Patrick McCrory, mayor of Charlotte, NC, and a member of the President's Homeland Security Advisory Council.

Source: <http://www.fcw.com/geb/articles/2004/0119/web-money-01-22-04 .asp>

[\[Return to top\]](#)

Emergency Services Sector

23. *January 22, Lamar Daily News (Lamar, CO)* — **Emergency planning committee eyes training drills.** A committee of Lamar, CO, emergency response officials met Wednesday, January 21, to outline plans for how to proceed with tabletop exercises and a full-fledged disaster drill in hopes of beefing up their ability to respond to disaster, including the possibility of terror-related incidents. The group, led by Prowers County Sheriff, is trying to untangle the

maze of new state and federal planning requirements, while at the same time attempting to sift through a maze of funding issues, but locals say it is unlikely any additional amounts of funding will be granted to rural areas. **To qualify for any Homeland Security–related funding assistance, any such drill would have to include terror related or weapons of mass destruction related training, and some believe that emergency response people are already versed in how to handle the more likely natural disasters, since they have faced such threats, have already trained for them, and have even been through a couple real life events.**

Source: <http://www.lamardaily.com/Stories/0.1413.121~7979~1908117.00.html>

[[Return to top](#)]

Information and Telecommunications Sector

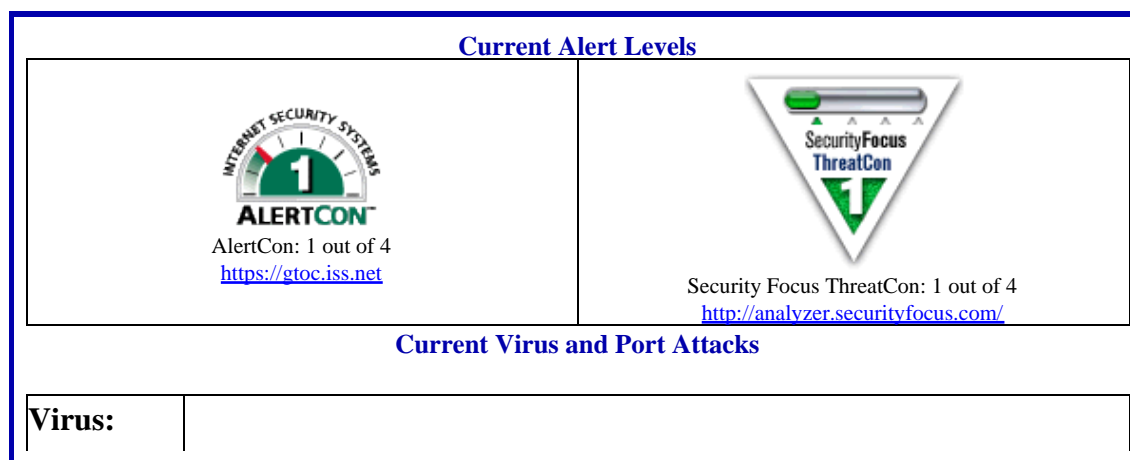
24. *January 22, earthweb.com* — **Cisco warns of voice product security flaws. Cisco on Thursday, January 22, warned of a default installation vulnerability in multiple voice products running on the IBM platform that leaves TCP and UDP ports open to malicious attack.** Cisco said the security flaw could be exploited to cause denial-of-service attacks and administrative takeover. According to the Cisco advisory, the vulnerable voice products running on IBM servers install the Director Agent insecurely by leaving the service on port 14247 (both TCP and UDP) accessible without requiring user authentication. In addition to leaving the products susceptible to administrative takeover, a malicious attacker could make the IBM Director Agent process consume a server's entire CPU resources by scanning it with a network scanner. This advisory underscores the risks that come with the growing dependence on IP-based networks, especially in the enterprise. Specific information on this advisory can be found at: <http://www.cisco.com/warp/public/707/cisco-sa-20040121-voice.shtml>
Source: <http://news.earthweb.com/dev-news/article.php/3302271>

25. *January 22, Government Computer News* — **Security analysts recommend scrapping online voting plans. A group of security analysts who have evaluated Department of Defense (DoD) plans for an online voting pilot have recommended that the plan be scrapped because its security cannot be ensured.** The analysts concluded "Internet voting presents far too many opportunities for hackers or even terrorists to interfere with fair and accurate voting." **The DoD, however, said it has no intention of stopping the program. "Security was our Number One priority when we started on this concept," DoD spokesman Glenn Flood said.** The Secure Electronic Registration and Voting Experiment (SERVE) is a DoD program being operated by the Federal Voting Assistance Program (FVAP) to ease absentee voting procedures for U.S. citizens living or serving overseas. A 10-member Security Peer Review Group put together by FVAP evaluated the system. A minority report was issued by four members of the group. The report said inherent flaws in proprietary software, the Internet and PCs from which votes would be cast make the process too risky to be used in a real election. Threats include insider flaws, denial-of-service attacks, spoofing attacks, and malicious code. Flood said weaknesses in the Internet infrastructure were taken into account in designing SERVE.
Source: http://www.gcn.com/vol1_no1/security/24681-1.html

January 21, eSecurityPlanet — **Sun Cluster vulnerable to OpenSSL flaw.** Sun Microsystems on Wednesday, January 21, warned that systems running Sun Cluster 3.x with SunPlex Manager configured were at risk of takeover because of known flaws in the OpenSSL protocol. In a security advisory, Sun recommended that the SunPlex Manager be disabled until a comprehensive patch is ready, warning that exploitation of the vulnerability could lead to arbitrary code execution and denial-of-service (DoS) scenarios. Independent research firm Secunia is rating the vulnerability as "moderately critical." The confirmation of the system access and DoS vulnerabilities comes more than three months after the OpenSSL flaw was made public. Last October, the OpenSSL Project released new versions of its implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to plug multiple vulnerabilities. All versions of OpenSSL up to and including 0.9.6j and 0.9.7b and all versions of SSLeay were updated. The OpenSSL project said any application that makes use of OpenSSL's ASN1 library to parse untrusted data was also susceptible. The OpenSSL holes carry a "highly critical" rating. More information can be found at <http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57475>
Source: <http://www.esecurityplanet.com/prodser/article.php/3301661>

27. *January 20, Federal Computer Week* — **Florida governor seeks IT funding overhaul.** Florida Governor Jeb Bush on Tuesday, January 20, outlined a 2004–2005 budget that calls for several changes at the State Technology Office (STO), including consolidating its funds to gain better control of cross-sector initiatives. This year, the STO's Information Technology Security Office is developing a statewide intrusion detection service, or Cyber Center, using funding from a federal grant. That service "will move the office into an expanded role to provide physical monitoring of the state's IT infrastructure to detect, prevent and minimize cybercrime," according to budget documents. Governor Bush requested almost \$1.1 million of the state's money to continue the security office's work. The new budget also reflects the STO's shift from legacy systems to Web-based services. Over all of this, the budget proposes a complete reorganization of the STO's programs into a single budget. "This realignment of budget authority within a single budget entity will provide the necessary flexibility for the State Technology Office to meet the needs of its IT partners and customers as needed, while also maintaining the requisite level of budgetary accountability."
Source: <http://www.fcw.com/geb/articles/2004/0119/web-florida-01-20-04.asp>

Internet Alert Dashboard



	#1 Virus in the United States: JAVA_BYTEVER.A Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 6129 (dameware), 1434 (ms-sql-m), 137 (netbios-ns), 80 (www), 445 (microsoft-ds), 4000 (Connect-BackBackdoor), 139 (netbios-ssn), 53 (domain), 1433 (ms-sql-s) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

[[Return to top](#)]

General Sector

28. *January 22, Reuters* — Musharraf sees al Qaeda behind assassination bids. President Pervez Musharraf said on Thursday, January 22, that Pakistan was investigating a "definite possibility" of al Qaeda involvement in two attempts to assassinate him last month. "We have unearthed a lot. We have in fact netted all the people directly involved in the action but we are trying to see who was behind them, the real links, as they say," Musharraf told reporters at the World Economic Forum in Switzerland. **"We think that yes, there is a definite possibility of some al Qaeda in the rear," either ordering or executing the attacks, he added.** "We are now trying to see the linkage with our (Pakistani) extremist organizations, we need to establish that still."

Source: http://www.reuters.com/locales/newsArticle.jsp?type=worldNews&locale=en_IN&storyID=4188631

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at

703–883–6631

Subscription and
Distribution Information

Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703–883–6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202–323–3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.